Propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas.

Proposal of a system of governance, risks and compliance to be aligned to different regulations in small and medium enterprises.

Felisa Yaerim López Botello
Universidad Autónoma del Estado de México
fely_yaerim@hotmail.com

Eréndira Garduño Pérez
Universidad Autónoma del Estado de México
chik_aries_05@hotmail.com

Araceli Romero Romero
Universidad Autónoma del Estado de México
chelitos_2@hotmail.com

Verónica Alvarado Campuzano
Universidad Autónoma del Estado de México
valvaradoc@uaemex.mx

Miguel Octavio Caballero Santín
Universidad Autónoma del Estado de México
miguel.ocs@gmail.com

Resumen

Las organizaciones buscan el cumplimiento de objetivos que provienen de las partes interesadas de la organización, el contexto en el cual existen y las regulaciones aplicables a su actividad.

Es necesario utilizar una visión holística para la implementación de la Gobernabilidad, Riesgos y Cumplimiento (GRC), es decir una visión que contemple los distintos aspectos organizacionales y el contexto externo e interno como un todo. Mapear los

procesos y controles con las regulaciones y esquemas de cumplimiento a los que debe apegarse la organización, medir y priorizar los riesgos para implementar medidas que permitan dar tratamiento adecuado y aseguren el cumplimiento de los objetivos organizacionales.

Este documento tiene como fin realizar una propuesta de un sistema informático de GRC adecuadamente diseñado e implantado que permita establecer una relación directa entre cada una de las actividades realizadas por la organización, sus métricas, los KPI, los objetivos de negocio y las expectativas de las partes interesadas, de forma que todos sean componentes de una sola maquinaria que busca una meta en común.

En el documento se revisan distintas herramientas que existen en el mercado y que permiten definir y dar seguimiento a esquemas de GRC, sin embargo, cada una tiene sus propias limitaciones, ventajas y desventajas, por lo que se decidió la creación de una ontología propia y el uso del *Semantic Web Builder* (SWB) para su uso diario.

El uso de SWB facilita la generación de una herramienta de GRC debido a que ya cuenta con un portal, una herramienta de diseño y módulos de importación y personalización que facilitan el desarrollo y mantenimiento de nuevos modelos ontológicos.

Derivado de lo anterior se recomienda la creación de una ontología adecuada a las necesidades de cada organización, que permita documentar, dar seguimiento y visualizar el esquema de Gobernabilidad, Riesgos y Cumplimiento de una organización. Esto, requiere del entendimiento de las relaciones entre los objetivos e indicadores en los distintos niveles y roles organizacionales identifica cómo éstos se aterrizan en actividades de los niveles inferiores de la jerarquía organizacional, así como en el sentido inverso se puede dar seguimiento al cumplimiento de dichos objetivos con base en las actividades.

Dado que el riesgo se define como "incertidumbre sobre los objetivos", el cumplimiento de cada uno de los requisitos impuestos por los intereses de las partes interesadas, apoya en la consecución de objetivos de un nivel superior o inferior y los riesgos están relacionados con las actividades que soportan cada objetivo.

Palabras clave: Gobernabilidad, Riesgos, GRC, KPI, PyME

Abstract

Organizations seek the fulfillment of objectives that come from the stakeholders of the organization, the context in which they exist and the regulations applicable to their activity.

It's advisable to use a holistic vision for the implementation of Governance, Risks and Compliance (GRC), i.e. a vision that contemplates the various organizational mechanisms and the external and internal context as a whole. Map processes and controls with regulations and compliance schemes and those that must meet the organization, measure and prioritize risks to implement measures that allow adequate treatment and ensure compliance with organizational objectives.

The objective of this document is to make a proposal for an appropriately designed and implemented GRC system that allows a direct relationship between each of the activities carried out by the organization, its metrics, KPIs, business objectives and expectations. The stakeholders, so that all are components of a single machinery that seeks a common goal.

The document reviews different tools that exist in the market, that allow to define and follow GRC schemes. However, each has its own limitations, advantages and disadvantages, so it was decided to create an own ontology and The use of *Semantic Web Builder* (SWB) for daily use.

The use of SWB facilitates the generation of a GRC tool because it already has a portal, a design tool and import and customization modules that facilitate the development and maintenance of new ontological models.

Derived from above, it's recommended to create an ontology that is appropriate to the needs of each organization, to document, monitor and visualize an organization's governance, risk and compliance framework. This requires the understanding of the relationships between objectives and indicators at different organizational levels and roles, identifying how they are landed in activities at the lower levels of the organizational hierarchy, and in the reverse sense based on the activities.

Key words: Governance, Risks, GRC, KPI, PyME.

Fecha recepción: Julio 2016 **Fecha aceptación:** Diciembre 2016

Introducción

"Para hacer frente a algunos problemas estratégicos, algunas organizaciones han desarrollado iniciativas conocidas como Gestión, Riesgos y Cumplimiento (GRC), las cuales permiten una revisión integral mediante sus funciones de riesgos y control, además de mejorar su eficiencia y eficacia". (J.Anderson, 2009)

La estrategia de negocio es fundamental para asegurar la permanencia y éxito de las organizaciones en un mercado cada vez más competitivo. Por ello, es necesario que esta estrategia sea apalancada por herramientas automatizadas que permitan la toma de decisiones, el control y la gestión de las actividades organizacionales para monitorear el desempeño y controlar los resultados que se derivarán de los planes de negocio, requisitos reglamentarios, regulatorios o legales.

La implementación y utilización de herramientas que permitan dar seguimiento a la Gestión de Riesgos y Cumplimiento proporciona beneficios como la gestión del conocimiento, la optimización de recursos, así como una mejor capacidad de respuesta y verificación del cumplimiento legal o regulatorio, lo que permite la entrega de servicios o productos eficaces y una mayor satisfacción del cliente.

Lo anterior se ve reflejado en la capacidad de una organización de dar trazabilidad al cumplimiento de sus objetivos, al Origen de dichos objetivos en los intereses de las partes interesadas y a su materialización en las actividades diarias de la organización.

En los últimos años, el incremento del mercado de software en México fue de 14 puntos porcentuales. Según datos de Select (SELECT, 2013), el aumento se debió a la demanda de soluciones tecnológicas de T.I. abocadas al procesado y análisis datos. Este estudio indica que entre 2012 y 2020 las áreas de TI mexicanas gestionarán 50 veces más información, lo que representa un enorme reto para la seguridad de la información y el almacenamiento de datos.

Según datos de la Dirección General de Normas, existen 1 749 empresas mexicanas con un sistema de gestión certificado, de las cuales menos del 1% cuenta con dos o más sistemas de gestión implementados e integrados. La mayoría de estas empresas gestionan su documentación de forma tradicional, es decir, mantienen su documentación en papel, lo que provoca que la información no cuente con los elementos de calidad antes

mencionados. Las principales causas son la sobre documentación de sus procesos y la falta de tiempo para la revisión y el mantenimiento de sus documentos. Adicionalmente, el sector de tecnologías de la información demanda la aplicación e integración con normas especializadas para este sector.

En la actualidad, existen en el mercado herramientas automatizadas especializadas en un solo estándar o proceso, lo que dificulta la integración de esas herramientas con otros estándares o bien requieren de una mayor inversión derivada de la necesidad de adquirir más herramientas.

En el sector de tecnologías de información (TI), la demanda de productos y servicios que cumplan con la calidad, los niveles de servicio acordados y los controles de seguridad que protejan la información y la privacidad de los datos personales se ha convertido en un requisito obligado si se pretende participar en proyectos privados y gubernamentales. Esto ha provocado la elaboración de normas tanto internacionales como nacionales, por ejemplo, las normas de Sistemas de Gestión especializadas en Tecnologías de Información como son: NMX-I-20000-1-NYCE, NMX-I-27001-NYCE, ISO/IEC 20000-1, ISO/IEC 27001 y la creación de nuevas leyes, como la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Actualmente las organizaciones del sector TI se enfrentan con la necesidad de atender los requisitos de negocio de la operación del producto o servicio que proporcionan, además de cumplir con los requisitos normativos, regulatorios o legales. Estos requisitos exigen mantener un Sistema de gestión cuya piedra angular es la generación de evidencia, así como su constante análisis y mejora, considerando los riesgos asociados al sector, la competencia y las debilidades de la organización.

Estas actividades significan una gran inversión de tiempo para el mantenimiento y control de información documentada, además de personal dedicado a las tareas de revisión, verificación y mejora constante.

Recientes estudios revelan que solo el 20% (ISO Survey, 2014) de las organizaciones con un sistema de gestión implementado logran mantenerlo por más de 3 años, y menos del 5% dan cumplimiento a más de dos referencias normativas. Una de las principales causas es la falta de tiempo y de recursos para la revisión y el mantenimiento constante.

Otro de los principales problemas para estas organizaciones es la falta de integración de su información documentada con todos los requisitos legales vigentes, debido a la actualización constante de los propios estándares y leyes, lo que en la mayoría de los casos eleva los costos para la contratación de personal extra que es necesario para la revisión y adecuación de los documentos.

Método

Sistemas de información estratégicos

Pueden considerarse como el uso de la tecnología de la información para respaldar o dar forma a la estrategia competitiva de la organización, al plan de ésta para incrementar o mantener su ventaja competitiva o bien para reducir la ventaja de sus competidores.

El crecimiento de las Tecnologías de la información y comunicaciones

Los flujos de información y la comunicación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva.

El de tecnologías de información y comunicaciones (TIC) es un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar y procesar información. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información.

Un estudio realizado por diversas organizaciones líderes en el sector (AMITI, CANIETI, FMD, 2006) indica que entre 2012 y 2020 las áreas de TI mexicanas gestionarán 50 veces más información, lo que representa un enorme reto para la seguridad de la información y el almacenamiento de datos.

Principales retos de empresas mexicanas

Las empresas mexicanas compiten no solamente con las empresas nacionales sino con aquellas que vienen del exterior, produciendo bajo diferentes sistemas financieros estados de derecho y una cultura laboral distinta, entre muchos otros factores que determinan la competitividad; se trata de una serie de elementos que además de multiplicarse, quedaron fuera del control de las empresas.

El Reporte Global de Competitividad 2012-2013 (Foro Económico Mundial, 2014) —elaborado anualmente por el Foro Económico Mundial (WEF, por sus siglas en inglés), organización con sede en Suiza— define la competitividad como el conjunto de instituciones, políticas y otros factores que determinan el nivel de productividad de un país.

Gobernabilidad

Para realizar un análisis de las deficiencias, se involucran tres áreas de la toma de decisiones: quién está gobernando, quién está siendo gobernado, y qué recursos o activos han de ser desplegados en el proceso. Los requisitos y la toma de decisiones se aplican a los gobiernos y las corporaciones por igual. La Ilustración 4 muestra las partes interesadas considerando ambos planos.

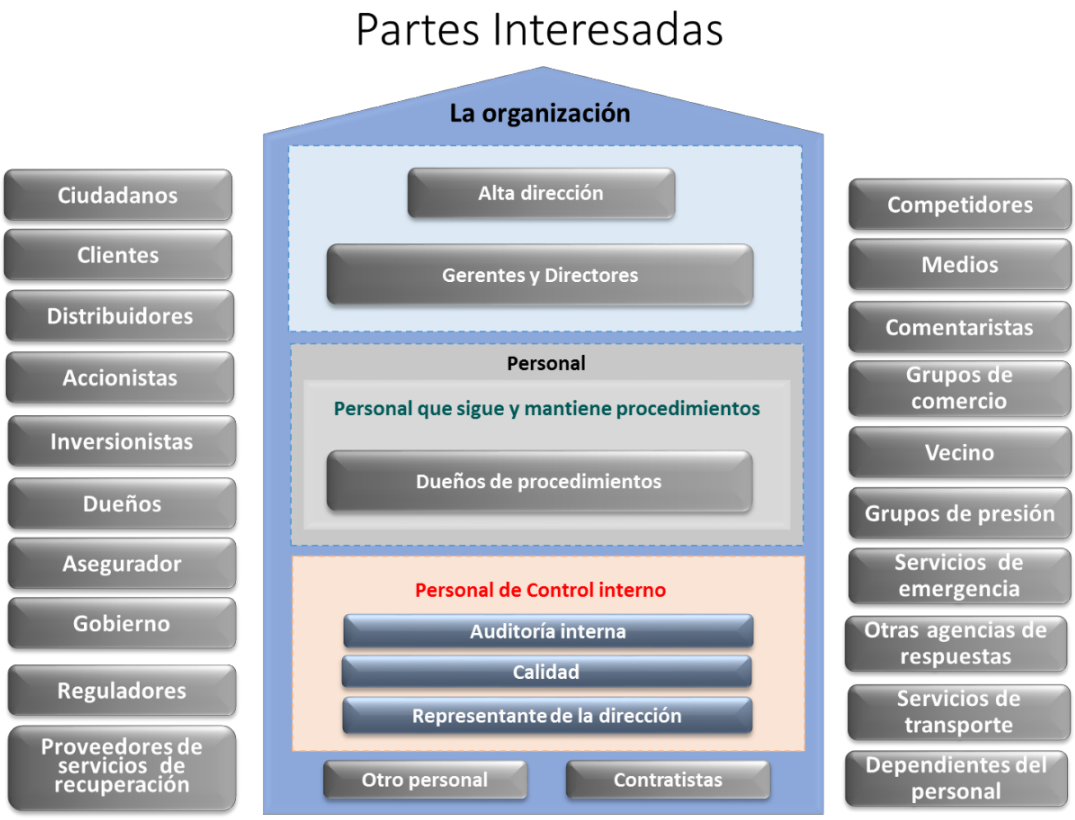

Ilustración 1. Partes interesadas. Adaptación del modelo de partes interesadas ISO 22301

Principios comúnmente aceptados de gobierno corporativo

Independientemente de las condiciones de la jurisdicción nacional y local, existen algunos principios (Tarantino, 2008) y temas de gobierno corporativo que han sido ampliamente adoptados a través de los años.

Derechos y trato justo de Accionistas. Las empresas tienen que escuchar las preocupaciones de los accionistas y respetar sus derechos. Esto incluye la comunicación abierta y bidireccional, así como la participación de los accionistas en las juntas directivas.

Funciones y responsabilidades de la Junta Directiva. Las juntas de gobierno corporativo robustas necesitan miembros expertos y enfocados que cuenten con cierto grado de experiencia. Es esencial contar con una mezcla de miembros independiente con credenciales fuertes y miembros internos con experiencia en la organización.

Comportamiento ético y profesional. Las empresas necesitan una cultura de cumplimiento y ética, no sólo un código de ética. Las voces de los directores se refuerzan por medio de acciones, no sólo con las palabras.

Transparencia y divulgación de información financiera. Las empresas necesitan procesos fuertes, bien documentados y de controles para proporcionar consistentemente una total transparencia en la información financiera. Los resultados necesitan seguir las normas aceptadas, las mejores prácticas y ser auditados por expertos internos y externos independientes. También es necesario defender y fomentar denunciantes internos, que a menudo son el mejor medio para descubrir errores y fraude en la información financiera.

Los controles internos son un componente clave de todos los regímenes para mejorar la gestión empresarial en general, para reducir los riesgos, y específicamente para proporcionar transparencia financiera consistente. Los debates sobre el alcance de los controles internos se han prolongado durante décadas, pero la mayoría está de acuerdo en que los controles internos que impactan en la caída de informes financieros están dentro del alcance del gobierno corporativo. En varios modelos para la gestión de riesgos se indica que la cuantificación y priorización de los riesgos es clave para el éxito de los controles.

Riesgos

La definición de riesgo comúnmente se refiere a la posibilidad de una pérdida o un daño creado por una actividad o por una persona. La gestión de riesgos busca identificar los activos o mediciones del riesgo para posteriormente desarrollar contramedidas para tratar o manejar el riesgo. Comúnmente esto no significa eliminar el riesgo, pero sí buscar mitigar o minimizar su impacto. El riesgo no debería verse como algo inherentemente malo. Todas las oportunidades vienen con algún grado de riesgo.

Una organización que es totalmente reacia al riesgo es probable que no sea muy atractiva para los inversionistas y puede ser condenada, en última instancia, al fracaso.

La norma ISO 31000 (ISO 31000, 2013), define como riesgo al efecto de incertidumbre sobre los objetivos; indica que un efecto es desviación esperada positiva y negativa, y los objetivos pueden tener diferentes aspectos como: financieros, de seguridad, de salud y ambientales, además de que pueden tener diferentes niveles como: estratégicos, organizacionales, por proyecto, por productos o por proceso. Los objetivos se caracterizan frecuentemente por asociarse a eventos potenciales y consecuencias o una combinación de estos, los cuales incluyen cambios en las circunstancias y una probabilidad de ocurrencia asociada.

Eventos

La norma define un evento como una ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas. Un evento también puede consistir en algo que no esté ocurriendo, y se identifica también como "incidente" o "accidente". Los riesgos pueden ser internos o externos.

Fuente del riesgo

Como se muestra en la Ilustración 8, un elemento o la combinación de varios elementos con potencial intrínseco para dar lugar a un riesgo se conoce como la "*fuente del riesgo*". Esta fuente puede ser tangible o intangible. Algunas fuentes de riesgos pueden ser: relaciones comerciales y legales, circunstancias económicas, comportamientos humanos, eventos naturales, circunstancias políticas, aspectos tecnológicos y técnicos, actividades organizacionales o actividades individuales, entre otros. Estos eventos pueden ser

positivos o negativos y pueden estar asociados a las partes interesadas, a las cuales se conoce como *"Agente del riesgo".*

Gestión del Riesgo

De acuerdo a la norma ISO 31000, la gestión de riesgos se define como las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo identificado.

La gestión de riesgos para la tecnología de la información (TI) es un reto cada vez mayor como requisito de cumplimiento, creciendo a un ritmo exponencial y con impacto en todas las áreas de TI. Las altas tasas de rotación para los Jefes de información (CIO) y los directores de tecnología (CTO) son evidencia de la creciente carga y tensión puesta en las organizaciones de TI. A medida que aumenta la presión sobre los responsables financieros, se hacen cada vez mayores las demandas de TI para mejorar la puntualidad, la exactitud y el costo de almacenamiento, de archivo, de cifrado, así como la búsqueda, la recuperación, la información financiera consolidada, las alertas, los documentos y la gestión de documentos, el correo electrónico y los controles de mensajería instantánea, etcétera.

La gestión de riesgos incluye el establecimiento del contexto, la identificación, el análisis, la evaluación, el tratamiento y el monitoreo del riesgo. La gestión de riesgos se utiliza principalmente en riesgos negativos.

Cumplimiento

Se define como cumplimiento el actuar en conformidad o de acuerdo a las leyes, regulaciones, protocolos o estándares establecidos. En México se cuenta con más de 800 Normas Oficiales Mexicanas (DGN, 2016) lo que significa que su cumplimiento es obligatorio. Adicionalmente, se cuenta con 289 leyes o regulaciones (DOF, 2014). El incremento de leyes y regulaciones se debe principalmente a la necesidad de proteger el bienestar de una nación y crecimiento económico. Por ello, el costo del incumplimiento es muy alto y puede tener consecuencias tangibles o intangibles.

Tratamiento

Las opciones para el tratamiento de riesgos dependen en gran medida de las circunstancias y del nivel de riesgos. La norma ISO 31000 establece opciones de tratamiento de riesgo:

- Evitar el riesgo decidiendo si se continúa con la actividad que da lugar a un riesgo. Esta opción se utiliza comúnmente para riesgos negativos;
- Tomando o incrementando el riesgo de manera que se persiga una oportunidad. Opción de tratamiento para riesgos positivos;
- Mitigar el riesgo, modificando la probabilidad o consecuencias mediante el establecimiento de medidas de control. Opción para riesgos positivos y negativos;
- Compartir el riesgo con otras partes, mediante contratos o pólizas. Opción comúnmente utilizada para riesgos negativos;
- Retener el riesgo, es decir no se realizan acciones y se informa a las partes interesadas sobre la existencia del riesgo; opción para riesgos positivos y negativos.

La selección más apropiada para la opción de tratamiento de riesgo involucra el balance de los costos y esfuerzos de implementación contra los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros.

La norma ISO/IEC 27001 (ISO 27001, 2013) establece la necesidad de elaborar un plan de tratamiento de riesgo, sin embargo, no existen requisitos normativos que indiquen qué elementos debería incluir este plan. Tarantino establece en su libro de gobernabilidad (Tarantino, 2008) que este plan debería contener información sobre:

- Descripción del riesgo
- Responsable del riesgo
- Controles asociados al riesgo
- Medidas de control (incluyendo documentación para su mantenimiento y control)
- Medición de su eficacia
- Resultado de la eficacia del control
- Referencias sobre las acciones correctivas o de mejora asociadas al riesgo

Esto ayuda a identificar claramente la relación entre la gestión del riesgo, la operación y la mejora de los controles asociados.

Eficacia

Los mecanismos para monitorear el control y la forma para medir su eficacia deberían estar documentados; para ello se identifica el indicador clave de desempeño, conocido como KPI, que puede estar relacionado a otros controles, incidentes o eventos significativos que pueden ocasionar un riesgo.

Herramientas para la Gestión de Riesgos de Cumplimiento

El manejo de sistemas de información es muy importante para los planes de la empresa. Contar con la tecnología adecuada es la parte fácil; el reto es adecuar la tecnología a las necesidades de la organización. Alcanzar un alto grado de adecuación es un aspecto principal para el éxito de la compañía. Cualquier decisión para invertir en algo de la empresa significa más que un compromiso de tiempo, esfuerzo y recursos financieros.

Actualmente existen en el mercado aplicaciones automatizadas que permiten el cumplimiento con alguno de estos estándares, sin embargo, no permiten su integración con otros requisitos ni actualización constante.

A continuación, se muestra un análisis de las herramientas existentes en el mercado que ayudan a la administración de un sistema de gestión de riesgos de cumplimiento:

Herramienta / Sitio	Descripción
SecureGRC https://www.egestalt.com/securegrc-ent.html	Solución integral de monitoreo de seguridad de TI y gestión de cumplimiento que simplifica y reduce el tiempo necesario para la vigilancia de la seguridad, el cumplimiento normativo y el proceso de certificación
ORCA GRC Suite http://www.gcpglobal.com/orca-descripcion.php	La diversidad de soluciones en prevención de riesgos que ofrece ORCA y el respaldo de expertos multidisciplinarios para la entrega de servicios consultivos le permite diferenciarse de la mayoría de sus competidores dando como resultado la optimización operativa, la reducción de costos y la simplificación de las operaciones, así como el mejoramiento de la visibilidad y la toma de decisiones para propiciar un Gobierno Corporativo más eficiente.
SoftExpert **GRC Suite** http://www.softexpert.es/gestion-gobierno-riesgos-reglamentaciones.php	Ofrece una estructura de gobernanza que posibilita una tomada de decisión eficaz y cambios comportamentales. Ofrece a la organización una implementación viable y eficiente de la gobernanza corporativa y de TI.
ARIS Risk & Compliance Manager http://www.softwareag.com/corporate/solutions/ebpm/grc/overview/default.asp	Software para eficientar la gestión de riesgo del cumplimiento.

Tabla 1. Comparativa de aplicaciones GRC

El desarrollo de la herramienta a la medida fue descartado por la dificultad que significa asumir el riesgo en cuanto a la seguridad y el aseguramiento de la calidad por parte del departamento de TI, quienes debido a la saturación de trabajo no podrían dedicar el tiempo suficiente a ello. Por otra parte, la contratación de una empresa que desarrolle el software a la medida supera en tiempo y costos las ofertas de los sistemas licenciados.

Conclusión

Si bien el sistema con mejores calificaciones es *ARIS Risk & Compliance Manager*, éste no brinda una plataforma que cumpla con los objetivos de flexibilidad, escalabilidad y tipos de relaciones que se requieren.

Por lo tanto, el diseño de un sistema que permita dar trazabilidad al cumplimiento de objetivos, identificando las actividades que se realizan, los roles, las responsabilidades, así como los datos de entrada y salida de cada una de ellas, aportaría valor de forma importante al seguimiento y al cumplimiento de los objetivos organizacionales. Para ello será necesario el uso de una plataforma que ya cuente con las características de seguridad y aseguramiento de calidad requeridas.

Los intereses de las distintas partes interesadas pueden relacionarse con cada uno de los objetivos a los distintos niveles organizacionales, hasta llegar a los más operativos. De igual manera estos objetivos pueden ser medidos por medio de indicadores que provienen de los resultados de esas actividades operativas y que permiten a los niveles superiores conocer el estado del cumplimiento de sus objetivos con respecto de los resultados de las actividades de los niveles que están por debajo de ellos.

Douglas R. Hofstadter en Gódel, Escher y Bach: Una esterna trenza dorada (Hofstadter, 1980) Capítulo 9: "Mumon and Gödel" dice:

“Relying on words to lead you to the truth is like relying on an incomplete formal system to lead you to the truth. A formal system will give you some truths, but as we shall soon see, a formal system, no matter how powerful—cannot lead to all truths.”

Basarse en palabras para encontrar la verdad es como basarse en un Sistema formal incompleto para llegar a la verdad. Un sistema formal nos dará algunas verdades, pero como veremos, un sistema formal, no importando qué tan poderoso, no puede darnos todas las verdades.

Esta es la razón por la que las redes semánticas pueden acercarse más a la representación de los esquemas de la vida real, más allá de los esquemas formales.

Resultados

Tipo de estudio

El tipo de estudio considerando su finalidad es aplicado, pues contribuye a la resolución de los problemas derivados del mantenimiento de cumplimiento con diferentes leyes, normas y regulaciones. El lugar de estudio fue *In situ*, puesto que se realizó dentro del organismo encargado de evaluar la conformidad de normas mexicanas relacionadas con las tecnologías de la información.

En cuanto a las fuentes de información, también consideradas como instrumentos, se consideran dos tipos:

Documental: Se consultaron diferentes metodologías y normas relacionadas con sistemas de gestión, aplicaciones automatizadas especializadas en la gestión, mejora continua, cumplimiento, gobernabilidad y riesgos.

De campo: Se consultaron diferentes estudios relacionados con las diversas problemáticas de organizaciones privadas y gubernamentales, primordialmente mexicanas, relacionadas con la gestión y mantenimiento de cumplimiento de las diferentes leyes normas y regulaciones en el sector de tecnologías de la información. Adicionalmente, se hizo un análisis de las diferentes aplicaciones existentes en mercado enfocadas a la gestión de cumplimiento.

El alcance de la investigación está enfocado a cuatro tipos:

Exploratorio: Se buscaron las diferentes posibles causas que provocan la falta de cumplimiento constante y sus consecuencias, las cuales estuvieron basadas en los estudios y las experiencias de los auditores encargados de evaluar la conformidad.

Descriptivo: El diseño de la metodología propuesta para la educación de la herramienta automatizada para resolver la falta de cumplimiento describe las propiedades y características de cada una las entidades.

Correlacional: La metodología propuesta describe las diferentes relaciones entre las diferentes entidades y sus variables.

Explicativo: Este ensayo intenta resolver la problemática mediante la identificación de su causa raíz.

El universo muestra en el que se basó este ensayo es el sector de tecnologías de la información del mercado mexicano, aunque para la investigación de las posibles soluciones se consultaron estudios internacionales. La selección de las variables de estudio está enfocada en:

La estructura de cumplimiento propuesta.

La identificación de los elementos que ayuden a mantener este cumplimiento y su relación con la estructura de cumplimiento.

La automatización de estos elementos por medio de una herramienta tecnológica.

Características con las que debe contar el "Sistema de cumplimiento múltiple"

- Flexibilidad para presentar la información
- Facilidad de uso para la captura de información
- Escalabilidad para crecer con los requerimientos de la organización y complejidad de esquemas de cumplimiento
- Capacidad de administrar relaciones de un nodo a muchos otros nodos

Se trata de obtener la representación del conocimiento que se posee sobre un dominio del saber determinado; por tanto, la primera tarea a realizar consiste en determinar con precisión el dominio de conocimiento elegido, después, descomponerle en sus partes y en los elementos considerados esenciales para su descripción y por último integrarlo mediante las relaciones significativas que se puedan establecer entre aquellas partes o elementos.

La representación adoptada utiliza redes semánticas, es decir, grafos orientados con etiquetas en los vértices y en los arcos. Los vértices representan las partes o elementos del dominio considerado y los arcos las relaciones establecidas entre ellos.

Establecimiento de métricas para el monitoreo del desempeño

Para poder monitorear el desempeño del proceso y la gestión es necesario establecer qué información se requiere para iniciar el proceso, conocer qué información genera o sus salidas, identificar qué se debe medir o informar por medio del establecimiento de métricas, mecanismos para medirlo e identificar aquellas métricas que sean clave para el

desempeño, es decir indicadores clave de desempeño, KPI, y finalmente establecer metas con respecto a los KPI identificados.

Establecimiento de acciones correctivas / preventivas

Con base en el monitoreo de los indicadores establecidos, es necesario implementar acciones que atiendan las desviaciones o que permitan realizar cambios en la organización que la lleven a la mejora continua.

- Quién
- Incumplimiento (referencia)
- Causa
- Actividades (responsable, fecha, recursos)
- Prioridad
- Cierre
- Verificación

Cuando el sistema haya presentado desviaciones con respecto a los Factores Críticos de desempeño, deberán implementarse acciones correctivas o preventivas. Las acciones correctivas deben tener un responsable que vele por que las acciones se lleven a cabo y se eliminen las desviaciones. Debe estar referenciado el requisito incumplido el cual puede ser una actividad, un proceso, un procedimiento, una ley o una regulación afectada; debe indicar la causa por la cual no se cumplió con el requisito; es necesario se establezca su nivel de importancia o prioridad y que incluya un plan de acción que cuente con actividades, responsables y los recursos que se requieren para llevarlo a cabo. Finalmente es necesario realizar y verificar si las acciones fueron realizadas.

El nivel de descripción de los requerimientos fue alineado a la definición de negocio de Wiegers (Wiegers, 2003), que los define como aquellos requerimientos que representan objetivos de alto nivel para la organización o el cliente que requiere el producto. Estos requerimientos son la necesidad principal por la cual se empieza la construcción o mejora del producto. Estos requerimientos se caracterizan por ser descritos de manera muy generalizada en términos de beneficios o necesidades de la organización y se expresan en un lenguaje natural. En ocasiones son llamados los objetivos del software. En

ese sentido la Tabla 14 describe los requerimientos no funcionales para el Sistema de Cumplimiento Múltiple.

REQUERIMIENTOS	DESCRIPCIÓN
DESEMPEÑO	El sistema debe estar disponible y funcionar dentro de la organización y desde cualquier navegador. Debe permitir
SEGURIDAD	El sistema debe controlar el acceso y privilegios de los administradores y usuarios. Debe proteger la integridad de los datos que procese el sistema y deben existir mecanismos que protejan la conexión con otros sistemas o base de datos. El sistema debe
ESCABILIDAD	El sistema debe permitir la adición de nuevas funcionalidades, modificar o eliminar las funcionalidades existentes.
FACILIDAD DE USO	El sistema debe ser intuitivo de manera que sea fácil de usar. El sistema debe emitir mensajes de error que permitan la
INTEROPERABILIDAD	El sistema debe permitir el intercambio y relación de información entre los diferentes módulos, base de datos y otros sistemas en tiempo real.

Tabla 2. Requerimientos de la herramienta de cumplimiento múltiple

SemanticWebBuilder se compone de un conjunto de herramientas que dan significado a la información obtenida de fuentes internas o externas, para su posterior integración, filtrado y presentación.

SemanticWebBuilder nos permitirá:

- Avanzar en la ruta Semántica hacia la Web 3.0.
- Incorporar elementos de colaboración como redes sociales, comunidades, blogs, wikis.
- Agilizar la implementación de portales con el uso de sitios predefinidos.
- Reducir los tiempos de desarrollo gracias a los componentes para crear aplicaciones basadas en modelos semánticos.

- Mejorar la clasificación y búsqueda de información para que pueda ser compartida entre diferentes organizaciones, estableciendo así una federación de información.

La ontología (lenguaje) de la plataforma incluirá elementos que podrán ser reutilizados para la creación de nuevos productos:

- Administración de usuarios (repositorios)
- Seguridad (reglas, roles, grupos y permisos)
- Navegación (sitios y páginas)
- Diseño gráfico (plantillas, diseño de interfaz)
- Administración de componentes (aplicaciones, contenidos, estrategias)
- Dispositivos
- Lenguajes

Uno de los elementos que se identificó como muy importante al momento de crear una ontología es el rol que juegan los activos en la organización. Existen distintas formas de clasificar los activos, en este caso serán definidos por la aportación al cumplimiento de los objetivos organizacionales, de forma que los que están directamente ligados a estos serán llamados activos primarios. Estos activos son los que dan valor a la organización y ayudan directamente al logro de los objetivos organizacionales y al cumplimiento de los intereses de las partes interesadas. Comúnmente pueden ser elementos no tangibles como:
Bases de datos, información, sistemas de tratamiento, personal, secretos del negocio, procesos operativos, resultados de la operación.

Los activos secundarios son aquellos que soportan a los activos primarios, ya sea como medios de almacenamiento, respaldo, transmisión, comunicación, procesamiento y hasta las instalaciones mismas donde se realizan las actividades organizacionales. Algunos ejemplos son: Personas, computadoras, servidores, archiveros, redes, nube, dispositivos móviles, respaldos, discos, expedientes.

Para la creación de la ontología se siguieron los pasos recomendados por (Noy & McGuinness, s.f.):

Determinar el dominio y el alcance de la ontología

¿Cuál es el dominio que cubrirá la ontología? La Gobernabilidad, Riesgos y Cumplimiento

¿Para qué vamos a usar la ontología?

Para el diseño de un sistema de Gobernabilidad, Riesgos y Cumplimiento soportado por una Red Semántica en una plataforma web.

¿Qué tipo de respuestas debe responder la ontología?

Qué relaciones existen entre los activos principales y secundarios de una organización. Cuál es la aportación que brinda cada activo al cumplimiento de los objetivos organizacionales. Cuáles son los riesgos asociados a los objetivos organizacionales y de qué forma son tratados mediante controles, actividades, políticas o proveedores.

¿Quién va a utilizar y dar mantenimiento a la ontología?

Deberá ser mantenida y adaptada a las necesidades de cada organización que busque implementarla.

Considerar la reutilización de otras ontologías

Se reutilizaron las ontologías swb.owl y swb.owl que son la base para el *Semantic Web Builder* creado por Infosec.

Listar los términos importantes en la ontología

- Esquema de cumplimiento
- Parte interesada
- Objetivo
- Riesgo
- Control
- Actividad
- Responsable
- Proveedor

Definir las clases y la jerarquía de clases.

Discusión y conclusiones

En el mercado existen distintas herramientas que permiten definir y dar seguimiento a esquemas de GRC, sin embargo, cada una tiene sus propias limitaciones, ventajas y desventajas, por lo que se decidió la creación de una ontología propia y el uso del *Semantic Web Builder* (SWB) para su uso diario.

El uso de SWB facilita la generación de una herramienta de GRC debido a que ya cuenta con un portal, una herramienta de diseño y módulos de importación y personalización que facilitan el desarrollo y mantenimiento de nuevos modelos ontológicos. Sin embargo es importante mencionar que si bien esta herramienta es más versátil y no requiere de una inversión inicial por costos de licenciamiento o pólizas de mantenimiento, es necesario que se inviertan recursos en conocer su funcionamiento, adaptarla a las necesidades organizacionales mediante la creación de nuevos modelos ontológicos, así como la definición y captura de los procesos organizacionales en la herramienta, lo que requiere de recursos, por lo que se recomienda que se analicen sus Costos totales de propiedad (PIERDANT, 2006) para asegurar su idoneidad.

La creación de una ontología adecuada a las necesidades de cada organización, que permita documentar, dar seguimiento y visualizar el esquema de Gobernabilidad, Riesgos y Cumplimiento de una organización, requiere del entendimiento de las relaciones entre los objetivos e indicadores en los distintos niveles y roles organizacionales identifica cómo éstos se aterrizan en actividades de los niveles inferiores de la jerarquía organizacional, así como en el sentido inverso se puede dar seguimiento al cumplimiento de dichos objetivos con base en las actividades.

Dado que el riesgo se define como "incertidumbre sobre los objetivos", el cumplimiento de cada uno de los requisitos impuestos por los intereses de las partes interesadas, apoya en la consecución de objetivos de un nivel superior o inferior y los riesgos están relacionados con las actividades que soportan cada objetivo.

Las relaciones que rigen la interacción entre los elementos descritos no siempre pueden ser definidas por medio de relaciones jerárquicas, por lo que fue necesaria la creación de otro tipo de relaciones que dieran flexibilidad a la interacción entre elementos.

Cada organización podrá reutilizar esta ontología para definir sobre ella nuevos elementos o nuevos tipos de relaciones que permitan definir elementos particulares de su contexto organizacional.

Futuros trabajos pueden centrarse en la integración de herramientas de medición y monitoreo automatizado, de forma que se pueda alimentar de manera sencilla la información que soporta la toma de decisiones. Por ejemplo herramientas como las propuestas por el National Isntitute for Standards and Technology (NIST) de los Estados Unidos de América, que han desarrollado el Security Content Automation Protocol (SCAP http://scap.nist.gov/revision/1.2/index.html) que es una serie

de especificaciones de interoperabilidad basada en una comunidad colaborativa abierta que ha desarrollado herramientas y listas de verificación para evaluar protocolos de seguridad informática.

No hay que olvidar que la ontología, incluyendo los elementos y los tipos de relaciones deberán ser adaptados a las necesidades de cada organización, de esta manera el sistema describe de forma precisa su realidad, los flujos de información, los roles y responsabilidades que rigen las actividades que realizan para la consecución de sus objetivos y a su vez el cumplimiento de las expectativas de las partes interesadas.

Bibliografía

AMITI, CANIETI, FMD. (2006). *Visión México 2020, Politicas Públicas en Materia de Tecnologías de Información y Comunicación para impulsar la competitividad de México.* Instituto Mexicano para la Competitividad, Select, CIDE.

Anderson, J. (1977). *Induction of augmented transition networks.* Cognitive Sciences.

Berners-Lee, T. (s.f.). *Semantic Web -XML2000 Architecture.* Obtenido de http://www.w3.org/2000/Talks/1206-xml2k-tbl/slide11-0.html

Beynon-Davies, P. (2002). *Modelo de la pirámide.*

Bobrow, D. e. (1973). *Representation and Understanding: Studies in Cognitive Science.* Academic Press.

Borkin, S. (1980). *Data models: a semantic approach for data base systems.* MIT Press. CoDD, E. (1979). *Extending the database relational model to capture more meaning.* ACM Transaction on Database Systems vol. 4, n. 4. Committee, C. P. (1971). *Databse Task Group Report.* ACM.

Cornella, A. (2000). *La gestión de la información en la organización.* Bilbao: Deusto. Dahl, O. D. (1972). *Structured programming.* Academic press.

Date, C. (1981). *An introduction to data base systems.* Addison-Wesley.

Deming, W. E. (1989). Calidad, Productividad y Competitividad: la salida de la crisis. Madrid: Ediciones Díaz de Santos.

DGN. (2016). *Catálogo de normas oficiales mexicanas*. Obtenido de http://www.economia.gob.mx/

DOF. (3 de Junio de 2014). *Leyes Federales Vigentes. Últimas reformas publicadas en el Diario Oficial de la Federación el 3 de junio de 2014.* Obtenido de http://www.diputados.gob.mx/LeyesBiblio/index.htm.

Fernandez, E. S. (1981). *Database security and integrity.* Addison-Wesley. Foro Económico Mundial. (2014). *Reporte de competitividad 2012 2013.* Garcia Camarero, E. (1980). *Garcia Camarero, E.* INRIA.

Garcia Camarero, E. V. (1980). *Seneca: Semantic networks for conceptual analysis. Data Bases in the Humanities and Social Sciences.* North-Holland.

Gruber, T. R. (1993). *A Translation.* Knowledge Acquisition.

Gruber, T. R. (1993). *Toward Principles for.* CA: Technical Report KSL-04, Knowledge Systems Laboratory, Stanford University.

Hofstadter, D. H. (1980). *Gödel, Escher, Bach: An Eternal Golden Braid.* Penguin Books. Imperio, M. d. (1965). *Data Structures and their Representation in Storage.* Pergamon press.

Institute for Electronics and Electrical Engineers. (1997). *Glosario estándar de la terminología de la ingeniería de software estándar 610.12-1990.*

ISO 27001. (2013). *ISO/IEC 27001 (2013), Information technology -- Security techniques -- Information security management systems – Requirements.*

ISO 31000. (2013). ISO 31000. En I. S. Organization.

ISO Survey. (2014). *Estudio ISO Survey.*

nderson, M. L. (2009). A Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*, 20, 22, 61.

Keilyn Rodríguez Perojo y Rodrigo Ronda León. (November-December de 2005). Web Semántica: un nuevo enfoque para la organización y recuperación de información en la web. *ACIMED, vol. 13, núm. 6, November-December* , http://bvs.sld.cu/revistas/aci/vol13_6_05/aci030605.htm.

Knuth, D. (1968). *The Art of Computer Programming.* Addison-Wesley.

Krech, D., Crutchfied, R., & Ballachey, E. (1975). indivíduo na sociedade. D.M. Lozada, A. (8 de Enero de 2016). *Semantic Web Builder*. Obtenido de Infotec:

http://www.semanticwebbuilder.org.mx/es_mx/swb/Ontologias

Noy, N. F., & McGuinness, D. L. (s.f.). *Ontology Development 101: A Guide to Creating Your First Ontology.* Obtenido de http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html

Objetivos SMART. (01 de 2016). Obtenido de https://en.wikipedia.org/wiki/SMART_criteria OCDE. (1989). Principios de Gobierno Corporativo.

Pariente, S. (2013). (A. Lozada, Entrevistador)

PIERDANT, E. (2006). *¿ QUÉ ES EL COSTO TOTAL DE PROPIEDAD?*

RAE. (2001). Diccionario de la Real Academia Española. RAE.

ScHANK, R. e. (1973). *Computer Models of Thought and Language.* Freeman.

SELECT. (2013). *Fortalecimiento y desarrollo de capacidades.* Secretaria de Economía. Shannon, C. e. (1949). *The mathematical theory of Comunication.* Universidad de Illinois. Somerville, I. (2004). *Ingeniería de software. 7 ed.* México: Addison – Wesley.

Tarantino, A. (2008). *Governance, Risk and Compliance Handbook.* Joh Wiley & Sons, Inc.

Taylor, R. e. (1976). *CODASYL Database management systems.* ACM Computing Survey, vol. 8, n. 1. Trost, H. e. (1981). *The Role of Roles: Some aspects of World Knowledge Representation.* IJCAI, .

W3C Working Group. (s.f.). Obtenido de Defining N-ary Relations on the Semantic Web: https://www.w3.org/TR/swbp-n-aryRelations/

Wiegers, K. (2003). *Software Requirements. 2 ed.* Washington: Microsoft Press. Winograd, T. (1983). *Language as a Cognitive Process, Vol. I: Syntax.* Addison-Wesley.